CYBERSECURITY (CYBR)

CYBR 100. Introduction to Computers 3 credits.
This course provides students with the ability to utilize and implement computer hardware and software into their cyber security and information technology endeavors. Students will analyze the principles of building, repairing, upgrading, and the common operating system principles of computers. The course will also emphasize the need for proper recording of documentation needed when working and making changes to a computer. Students will learn the integration, troubleshooting, and maintenance techniques of combining hardware and software. This also includes how the hardware is relevant towards the operation of computer's operating system. The importance of safety, privacy, and professionalism needed when working with computers and the individual that operate them.

CYBR 110. Introduction to Networking 3 credits.
This course provides students with the ability to utilize and implement computer networking into their cyber security and information technology endeavors. Students will analyze the principles of the OSI model, protocols, hardware, device configuration, management, security, and troubleshooting methods of networking. The course will also emphasize the need for proper recording of documentation needed when working and making changes to an organization's network. Students will explore and critically examine networks and the network's functions. Students will obtain the importance of safety, privacy, and professionalism needed when working with networks.

CYBR 120. Introduction to Security 3 credits.
This course provides students with the ability to utilize and implement computer and network security into their cyber security and information technology endeavors. Students will analyze the principles of the threats, policies, penetration testing, Bring Your Own Device (BYOD) security, security architecture, securing data, and troubleshooting methods of computer and networking security. The course will also emphasize the need for proper recording of documentation needed when working and making changes to enhance an organization's network. Students will obtain the importance of safety, privacy, and professionalism needed when working with computers and networks and the individuals that adhere towards the need of its security.

CYBR 310. Cybersecurity Strategy 3 credits.
This course is designed to cover the strategic, operational, and tactical aspects of the conflicts in cyberspace today. This course will provide a valuable resource to those involved in cyber warfare activities regardless of whether their focus is policy maker, CEO, CISO, doctrinal development, penetration testers, security professionals, network and systems administrators, or college instructors. The information provided on cyber tactics and attacks can also be used to assist in engineering better and more efficient procedures and technical defenses.

CYBR 320. Ethical Hacking & Countermeasures 3 credits.
The Certified Ethical Hacker program is the pinnacle of the most desired information security training program any information security professional will ever want to be in. To master the hacking technologies, you will need to become one, but an ethical one! The accredited course provides the advanced hacking tools and techniques used by hackers and information security professionals alike to break into an organization. As we put it, "To beat a hacker, you need to think like a hacker". This course will immerse you into the Hacker Mindset so that you will be able to

defend against future attacks. The security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment.

CYBR 330. Incident Handler 3 credits.
The Incident Handler program is designed to provide the fundamental skills to handle and respond to the computer security incidents in an information system. The course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats. Students will learn how to handle various types of incidents, risk assessment methodologies, and various laws and policy related to incident handling. After attending the course, they will be able to create incident handling and response policies and deal with various types of computer security incidents.

CYBR 340. Security Analysis 3 credits.
The Security Analyst training program is an information security training class designed to enable Security Professionals the advanced uses of the available methodologies, tools and techniques expected from a premier vulnerability assessment training and are required to perform comprehensive information security pen tests. Students will learn how to design, secure and test networks to protect any organization from the threat hackers and crackers pose. By enabling the Penetration Tester methodology and groundbreaking techniques for security and penetration testing, this will help you perform the intensive assessments required to effectively identify and mitigate risks to the security of organization's infrastructure. As students learns to identify security problems in this vulnerability assessment training certification course, they also learn how to avoid and eliminate them, with the class providing complete coverage of analysis and network security-testing topics.

CYBR 410. Certified Information Systems Security Professional – Phase I 3 credits.
The CISSP course helps individuals who have the ability, knowledge, and experience to implement solid security practices, perform risk analysis, identify necessary countermeasures, and help the organization protect its facility, network, systems, and information. The CISSP course also provides security professionals with the credential that represents the skill set they want to offer to employers. Today, a greater demand is put on security as an integral part of corporate success. This, in turn, increases the demand for highly skilled security professionals. This course, broken down into a phase 1 and subsequent phase 2 course, is aligned to the eight (8) domains of Information System Security Certification Consortium (ISC2).

CYBR 415 Certified Information Systems Security Professional – Phase II 3 credits. This is Part II of The CISSP course helps individuals who have the ability, knowledge, and experience to implement solid security practices, perform risk analysis, identify necessary countermeasures, and help the organization protect its facility, network, systems, and information. The CISSP course also provides security professionals with the credential that represents the skill set they want to offer to employers. Today, a greater demand is put on security as an integral part of corporate success. This, in turn, increases the demand for highly skilled security professionals. This course, broken down into a phase 1 and subsequent phase 2 course, is aligned to the eight (8) domains of Information System Security Certification Consortium (ISC2). The course contained, here-in, is the second phase. Prerequisite: CYBR 410.

Return to Table of Contents

CYBR 440. Advanced Security Trends 3 credits. This course provides students with the ability to explore and examine emerging trends and technology in cyber security. Students will analyze organizations and review the feasibility of adopting new cyber security policies to provide competitive advantages in the workplace. This course also evaluates how policies and procedures continue to evolve as technology workplace data security requirements change.

CYBR 450. Cybersecurity Capstone 3 credits. The cyber capstone course aims to give students hands-on experience, building on what they have learned during the specialization courses. The task of the Capstone is to design and build a secure system and expose weaknesses in systems built by other teams. The capstone follows the format of the Build-it Break-it Fix-it security contest. The Build it -Break it -Fix it security contest aims to teach students to write more secure programs. The contest evaluates participants' abilities to develop secure and efficient programs. The contest is broken up into three rounds. During the Build It round, builders write software that implements the system prescribed by the contest. In the Break It round, breakers find as many flaws as possible in the Build It implementations submitted by other teams. During the Fix It round, builders attempt to fix any problems in their Build It submissions that were identified by other breaker teams. Students are also supposed to submit a comprehensive case study pertaining to current IT cyber security policy. Participating in the course gives learners the chance to be part of research on understanding how to better build secure software. Prerequisite: CYBR 415